(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06195024 A**

(43) Date of publication of application: **15.07.94**

(51) Int. Cl **G09C 1/00**
H04B 7/26

(21) Application number: **04267811**

(22) Date of filing: **11.09.92**

(30) Priority: **13.09.91 US 91 759311**

(71) Applicant: **AMERICAN TELEPH & TELEGR CO <ATT>**

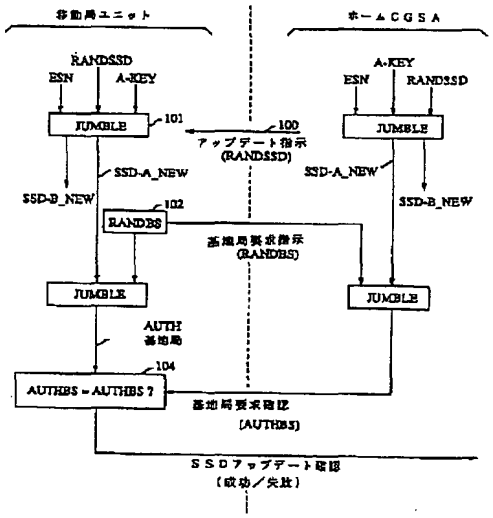
(72) Inventor: **REEDS III JAMES A**
TREVENTI PHILIP A

(54) AUTHENTICATING METHOD FOR OPENING COMMUNICATION CHANNEL AND MOBILE MACHINE

(57) Abstract:

PURPOSE: To obtain a public key authentication protocol which can be efficiently executed at high speed with hardware of kinds currently used for a cellular telephone by giving a hash authentication string to a base station, when a mobile station unit enters in the cell of the base station and giving a shared secret data field to the base station, when a center station judges it correct.

CONSTITUTION: The mobile station unit transmits its area code MIN 2 and telephone number MIN 1 designations to the base station and requests the base station to start the authentication process. A hashing function or a unidirectional function is used, in order to execute authentication process. MIN 1 designation and a secret key are installed, a cellular service area CGSA processor transmits a specified random sequence RANDSSD to the mobile station unit, and the generation of shared secret data SSD is indicated, so that the unit of a user is initialized. CGSA transmits RANDSSD and the generation of an SSD field, through the base station of the cell where the mobile station unit exists.



(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号

第2675494号

(45)発行日　平成９年(1997)11月12日　(24)登録日　平成９年(1997)７月18日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	６７３Ｂ	
Ｈ０４Ｑ　7/38			Ｈ０４Ｂ　7/26	１０９Ｓ	

請求項の数７(全 13 頁)

(21)出願番号　特願平4－267811

(22)出願日　平成４年(1992)９月11日

(65)公開番号　特開平6－195024

(43)公開日　平成６年(1994)７月15日

(31)優先権主張番号　７５９３１１

(32)優先日　1991年９月13日

(33)優先権主張国　米国（ＵＳ）

(73)特許権者　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(72)発明者　ジェームス　アレキサンダー　リーズ　サード
アメリカ合衆国　07974　ニュージャージー　ニュープロヴィデンス、サウスゲート　ロード　127

(74)代理人　弁理士　三俣　弘文

審査官　杓名　一夫

最終頁に続く

(54)【発明の名称】　通信チャネルを開設するための認証方法および移動機

1

(57)【特許請求の範囲】

【請求項１】　秘密情報コード列を保持する移動機によって実行される、基地局との通信チャネルを開設するための認証方法において、

基地局からディジタル乱数信号列を受信する受信ステップと、

前記秘密情報コード列、前記ディジタル乱数信号列、および、移動機を特徴づけるビット列を含むストリングを生成する生成ステップと、

ハッシュストリングを生成するために前記ストリングをハッシュするハッシュステップと、

前記ハッシュストリングを基地局へ送信するハッシュストリング送信ステップと、

要求ストリングを作成するステップと、

前記要求ストリングを基地局へ送信する要求ストリング

2

送信ステップと、

前記要求ストリング、移動機を特徴づける前記ビット列、および、前記ハッシュストリングの少なくとも一部からなる認証ストリングを形成するステップと、

前記認証ストリングをハッシュしてハッシュ認証ストリングを形成するステップと、

前記要求ストリング送信ステップに応答して確認ストリングを受信するステップと、

受信した確認ストリングを前記ハッシュ認証ストリングと比較するステップと、

前記比較ステップの結果を基地局へ送信するステップとからなることを特徴とする、通信チャネルを開設するための認証方法。

【請求項２】　移動機が基地局の管轄内に入ったことを判定するステップをさらに有することを特徴とする請求

項１の方法。

【請求項３】　基地局が移動機の再認証を必要とする場合に、前記受信ステップ、生成ステップ、ハッシュステップ、および、ハッシュストリング送信ステップを開始するステップを含むことを特徴とする請求項１の方法。

【請求項４】　秘密情報コード列を保持する移動機によって実行される、前記秘密情報コード列に関する知識を有しない基地局との通信チャネルを開設するための認証方法において、

基地局からディジタル乱数信号列を受信するステップと、

次の（１）、（２）、（３）および（４）を含むストリングを生成するステップと、

（１）前記移動機を特徴づけるビット列からなる部分ストリング、

（２）前記移動機によってなされる指定された作用に関係する部分ストリング、ただしこの部分ストリングは次の（ｉ）、（ｉｉ）および（ｉｉｉ）からなる集合から選択される、

（ｉ）空ストリング、

（ｉｉ）前記移動機に割り当てられた番号に対応するビットストリング、

（ｉｉｉ）接続しようとしている他の移動機の番号に対応するストリング、

（３）前記ディジタル乱数信号列からなる部分ストリング、

（４）前記秘密情報コード列から導出されたキーからなる部分ストリング、

ハッシュストリングを生成するために前記ストリングをハッシュするステップと、

前記ハッシュストリングを基地局へ送信するステップと、

要求ストリングを作成するステップと、

前記要求ストリングを送信する要求ストリング送信ステップと、

前記要求ストリング、移動機を特徴づける前記ビット列、および、前記ハッシュストリングの少なくとも一部からなる認証ストリングを形成するステップと、

前記認証ストリングをハッシュしてハッシュ認証ストリングを形成するステップと、

前記要求ストリング送信ステップに応答して確認ストリングを受信するステップと、

受信した確認ストリングを前記ハッシュ認証ストリングと比較するステップと、

前記比較ステップの結果を基地局へ送信するステップとからなることを特徴とする、通信チャネルを開設するための認証方法。

【請求項５】　基地局と通信する移動機において、該移動機は、

前記基地局との間に通信チャネルを開設し維持する際に使用するプロトコルで定められる制御信号を生成する制御信号生成手段（２００）と、

データ信号を生成するデータ信号生成手段（２００）と、

前記通信チャネルを通じて送受信する送受信手段（２２０）と、

前記移動機を特徴づけるビット列を格納する移動機識別レジスタ手段（２４０）と、

前記基地局から前記送受信手段を通じて受信されるディジタル乱数信号列を格納する一時レジスタ手段（２４０）と、

秘密情報コード列を格納するメモリ手段（２３２）と、

入力されるストリングをハッシュしてハッシュ出力を生成するハッシュ手段（２３１）と、

前記制御信号生成手段、データ信号生成手段、送受信手段、移動機識別レジスタ手段、一時レジスタ手段、メモリ手段およびハッシュ手段に接続されたプロセッサ（２１０）とからなり、該プロセッサは、

前記メモリ手段内の秘密情報コード列と、前記一時レジスタ手段内のディジタル乱数信号列と、前記移動機識別レジスタ手段内のビット列とからなるストリングを生成して前記ハッシュ手段に入力し、該入力に応答したハッシュ手段の出力であるハッシュストリングを、前記制御信号生成手段によって生成される制御信号とともに前記送受信手段に送って前記基地局へ送信させ、

前記データ信号生成手段によって生成された要求ストリングを前記制御信号生成手段によって生成される制御信号とともに前記送受信手段に送って前記基地局へ送信させ、

前記要求ストリングと、前記移動機識別レジスタ手段内のビット列と、前記ハッシュストリングの少なくとも一部とからなる認証ストリングを生成して前記ハッシュ手段に入力し、該入力に応答したハッシュ手段の出力であるハッシュ認証ストリングを前記制御信号生成手段によって生成される制御信号とともに前記送受信手段に送って前記基地局へ送信させ、

前記送受信手段が確認ストリングを受信したことに応答して、該確認ストリングを前記ハッシュ認証ストリングと比較し、該比較の結果を前記制御信号生成手段によって生成される制御信号とともに前記送受信手段に送って前記基地局へ送信させることを特徴とする移動機。

【請求項６】　前記メモリ手段の少なくとも一部が取り外し可能モジュール内にあることを特徴とする請求項５の移動機。

【請求項７】　前記モジュールは、電磁結合によって前記プロセッサに接続されることを特徴とする請求項６の移動機。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、認証プロトコルに関

し、特に、セルラ無線電話などの通信の妥当性を保証するためのプロトコルに関する。

【０００２】

【従来の技術】従来の電話においては、各電話端末（ファックス、モデム等）は、ローカルセントラルオフィス（端局）の交換機の１つのポートに、物理的に接続される。接続は、与えられた電話線あるいは電話線の指定のチャネルを介して行われる。電話線の接続はサービス提供者（通常は通信事業者）によって行われ、従ってサービス提供者は、チャネル上の通話が特定の加入者によるものであることを確信できる。一方、無線電話での加入者の認証は不確かなものである。

【０００３】米国における現在のセルラ電話方式では、加入者がセルラ電話で発呼を行うと、課金のためそのセルラ電話がサービス提供者に発呼者の身元を通知する。この情報は暗号化されていない。第三者がその時点で盗聴すると、加入者の身元情報が得られてしまう。この情報には、加入者の電話番号および加入者の装置のシリアル番号（ＥＳＮ）が含まれている。従って、盗聴者はセルラ電話をプログラムして正式な加入者になりすまし、サービスを受けることが可能となる。あるいは、他人の通話中に割り込んで、より強い送信電力で送信を行い、サービス提供者にある制御コードを送って接続に侵入することもできる。サービス提供者は、接続時および／あるいは通話中の発信者の身元の確認機構を持たないため、このような侵害は基本的に避けられない。

【０００４】盗聴者が身元情報を知ろうとすれば、セル内の全セルラ周波数帯を、自動的に走査する装置を用いることができる。従って、セルラ電話サービスの侵害を阻止できない。また、音声信号を暗号化していないため、会話の内容を盗聴することができる。つまり、セルラ電話システムにおいて効果的な保護手段が必要とされており、利用者の認証およびプライバシー保護のために、暗号化の利用が必要とされる。

【０００５】

【発明が解決しようとする課題】いくつかの標準的な暗号化方法は、セルラ電話等の一般的な認証問題の解決に用いることができるが、実際上の問題もある。まず、プライベートキー（秘密鍵）暗号アルゴリズムに基づいた、従来の要求／応答プロトコルを用いることができる。この方法では、加入者の移動ステーションに秘密キーが割り当てられ、このキーはホームシステムにも登録されている。サービス提供システムが加入者を認証する場合には、ホームシステムに対して、その加入者の場合に使用する要求ストリングおよび応答ストリングを申請する。ホームシステムはランダムな要求ストリングを作成し、加入者のキーと要求ストリングに対して一方向性関数を適用して、対応する応答ストリングを得る。これらの要求ストリングおよび応答ストリングはサービス提供システムに送られ、サービス提供システムは移動ステーションへその要求ストリングを送る。移動ステーションは、その要求ストリングと、記憶している秘密キーとから計算した応答ストリングを返す。サービス提供システムは、ホームシステムおよび移動ステーションからの応答ストリングを比較し、一致した場合に認証されたと見なす。

【０００６】この方法の問題点は、サービス提供システムが、発呼時の認証の際に、十分早くホームシステムに接続することができず、ホームシステムのデータベースソフトウェアが加入者の秘密キーを調べ、要求／応答ペアを構成することを短期間に行うことができない点である。ネットワークあるいはソフトウェアの数秒の遅延は、加入者が発信する際に、受話器を持ち上げてからダイヤルトーンが聞こえるまでのデッドタイムを増し、さらに（セルラ提供者の現在用いている制御ネットワークおよび交換装置では）遅延時間が増す。現状では、そのような遅延は許容されない。

【０００７】パブリックキー（公開鍵）暗号システムは、認証問題を解決するもう一つの標準的な方法である。一般的に、各移動ステーションはサービス提供者のパブリックキーによって、“パブリックキー証書”が与えられる。これは、その移動ステーションがサービス提供者の合法的な利用者であることを示すものである。さらに、各移動局に秘密データ（プライベートキー）が与えられる。移動局は、証書と同時にプライベートキーを用いて第三者に対し合法的な利用者であることを示す。

【０００８】例として、サービス提供システムはＲＳＡキーペア（Ｆ，Ｇ）を、Ｆをプライベート、Ｇをパブリックとして有する。サービス提供システムは各移動局に、そのＲＳＡキーの独自のペア（Ｄ，Ｅ）を、Ｆ（Ｅ）（サービス提供システムのプライベートキーＦを用いて移動局のパブリックキーＥを暗号化したもの）とともに与える。移動局は、サービス提供システムに、（Ｅ，Ｆ（Ｅ））を送ることによってその身元を提示する。サービス提供システムでは、Ｆ（Ｅ）にＧを適用してＥを得る。サービス提供システムは要求Ｘを生成し、移動局のパブリックキーＥを用いて暗号化してＥ（Ｘ）を得て、それを移動局へ送る。移動局は、Ｅ（Ｘ）にプライベートキーＤを用いてＸを得て、解読した状態でそれを応答としてサービス提供システムへ返送する。

【０００９】この問題について、処理あるいはデータ伝送量を減少させる改良例もあるが、セルラ電話で現在用いられているハードウェアにおいて、数秒以下で効率的に実行できる、パブリックキー認証方法は存在しない。認証時には、サービス提供システムとホームシステム間でのネットワークの接続性は必要とされないが、従来方法での時間的な制限が問題となるように、パブリックキー方法でも同様の制約が生じる。

【００１０】

【課題を解決するための手段】セルラ電話技術のセキュ

リティ需要は、共有秘密データフィールドによる方式によって満たされる。移動局ユニットは、サービス提供者によってそれに割り当てられた秘密を保持し、その秘密から共有秘密データフィールドを生成する。サービス提供者もその共有秘密データフィールドを生成する。移動局ユニットが基地局のセルに入ると、自分自身を基地局に認知させ、ハッシュストリングを基地局に送る。基地局は提供者に問い合わせ、その移動局ユニットが正当な装置であると判定された場合、提供者は基地局に共有秘密データフィールドを提供する。その後、移動局ユニットは、共有秘密データフィールドを使用して、移動局ユニットと基地局の間で実行される認証プロセスの助けを借りて、基地局と通信する。この方式の１つの特徴は、異なる基地局は、提供者によって移動局ユニットに組み込まれた秘密へのアクセス許可を有しないことである。移動局ユニットとの対話に成功した基地局のみが共有秘密データフィールドを有する。また、その数は、提供者が、単に、新たな共有秘密データフィールドを作成するよう移動局ユニットに指示することにより、制限することができる。

【００１１】この方式のもう１つの特徴は、秘密を使用する、より入念な認証プロセスは、時間がかかり、提供者が関わる場合にのみ起こるが、これは、移動局ユニットが最初にセルに入るとき（または共有秘密データフィールドが損傷を受けた疑いがあるとき）であり、頻繁には起こらない。

【００１２】呼の発信、呼の着信、およびその他の機能は、本質的に同一の認証プロトコルおよび同一のハッシュ関数を使用して認証される。ハッシュされる情報に若干の相違が現れる。

【００１３】

【実施例】移動セルラ電話システムは、多数の移動電話、少数のセルラ無線提供者（各提供者が複数の基地局を有する）、複数の交換ネットワーク提供者（通信事業者）から構成される。セルラ無線提供者と通信事業者は、セルラおよび非セルラ両方の電話加入者とのセルラ電話加入者による通話を可能にするように組み合せられる。図１に概略の構成を示すように、通信事業者ＩおよびＩＩは、交換機１０－１４を有する交換ネットワークを形成して結合される。固定局ユニット２０および２１は交換機１０に接続され、移動局ユニット２２および２３は不特定位置にあり、基地局３０－４０は交換機１０－１４に接続される。基地局３０－３４は提供者１、基地局３５および３６は提供者２、基地局３７は提供者４、基地局３８－４０は提供者３にそれぞれ属する。本発明の目的では、基地局とは複数の送信器を有するセルと同じ意味である。セルの集合体は、図１の基地局３０、３１および３２のように、地理上のセルラサービスエリア（ＣＧＳＡ）を形成する。

【００１４】各移動局ユニットは、そのユニット固有のシリアル番号（ＥＳＮ）を有する。ＥＳＮ番号はユニットの製造時に、製造者によって割り当てられ（例えば、ＲＯＭ内に）、アクセスはできるが変更はできない。

【００１５】利用者がその移動電話ユニットのサービスアカウントを申請すると、サービス提供者は利用者に、電話番号（ＭＩＮ１指定）、エリアコード（ＭＩＮ２指定）、“秘密キー”（Ａキー）を割り当てる。ＭＩＮ１およびＭＩＮ２指定は提供者のＣＧＳＡに関連し、図１の構成の全基地局は、特定のＭＩＮ２およびＭＩＮ１ペアの属するＣＧＳＡを識別することができる。Ａキーは、利用者装置および提供者のＣＧＳＡプロセッサ（図１には示さず）だけが知っている。ＣＧＳＡプロセッサは、ユニットのＥＳＮ、Ａキー、ＭＩＮ１およびＭＩＮ２指定の他、サービス提供者の必要な情報を保持している。

【００１６】ＭＩＮ１指定、ＭＩＮ２指定およびＡキーがインストールされ、ＣＧＳＡプロセッサが、移動局ユニットに特定のランダムシーケンス（ＲＡＮＤＳＳＤ）を送信し、“共有秘密データ”（ＳＳＤ）の作成を指示することによって、利用者のユニットが初期化される。ＣＧＳＡは、ＲＡＮＤＳＳＤと、ＳＳＤフィールド作成指令とを、移動局ユニットの存在するセルの基地局を通して送信する。ＳＳＤフィールドの作成は図２に示されるプロトコルに従う。

【００１７】図１の構成では、各基地局は、あらかじめ割り当てられたいくつかの周波数チャネル（ブロードキャストバンド）を用いて、そのセル内のすべてのユニットに情報を送信する。さらに、各移動局ユニットに対して、相互に確認した、（一時的に）割り当てられたチャネルによって、双方向通信を確保する。基地局と移動局ユニットで、通信チャネルの確認を行う方法は、本発明には重要でないため、ここでは詳しく述べない。例としては、移動局ユニットが全チャネルをスキャンし空きチャネルを選択する方法が考えられる。その後基地局へ、そのＭＩＮ２およびＭＩＮ１指定を送信し（平文で、あるいは、パブリックキーによって暗号化して）、基地局に認証プロセスを開始させる。認証された通信が確立されると、基地局は移動局を他のチャネルへスイッチしても良い。

【００１８】本発明による移動電話システムでの呼接続の確立と保持方法では、認証プロセスは会話中に多数回行われる。従って、認証プロセスは比較的安全で簡単に行うことができなければならない。設計を簡単にし導入費用を抑えるために、移動局ユニットおよび基地局の両方で同じプロセスを用いるべきである。

【００１９】多くの認証プロセスは、このプロセスを行うために、ハッシュ関数あるいは一方向性関数を用いる。ハッシュ関数は、“秘密キー”を署名に変換する、多対一のマッピングを実行する。以下に、簡単で、速く、効果的で、柔軟性のあるハッシュ関数の一例を示

す。これは、本発明の認証プロセスに好都合であるが、他のハッシュ関数を用いることもできる。

【００２０】［ジャンブルプロセス］

ジャンブルプロセスでは、ｄ個の“秘密”データワードｂ（ｉ）（ｉ＝０，１，...，ｄ－１）からなるブロックに対する署名を、ｋワードのキーｘ（ｊ）（ｊ＝０，１，...，ｋ－１）によって生成する。ここで、ｄ，＊

$s_d(t)=t$　　（$0 \leqq t \leqq d-1$）

$s_d(t)=2d-2-t$　　（$d \leqq t \leqq 2d-3$）

$s_d(t)=s_d(t+2d-2)$　　（すべてのｔに対して）

この関数は、ｚ＝０およびｉ＝０から開始され、０≦ｉ≦６ｄ－５の範囲で１ずつ増加する整数ｉに対する以下※

（ａ）　ｂ（s_d（ｉ））を、

$b(s_d(i))=b(s_d(i))+x(i_k)+SBOX(z) \mod 256$

によって更新する。ここで、

$i_k=i \mod k$

$SBOX(z)=y+[y/2048] \mod 256$

$y=(z(+)16)(z+111)(z)$

である。［ｙ／２０４８］はｙを２０４８で割った整数部を示し、（＋）はビットごとの排他的ＯＲ演算子である。

（ｂ）　ｚを、

$z=z+b(s_d(i)) \mod 256$

によって更新する。

＊ｉ，ｊ，およびｋは整数である。“署名”の生成プロセスは、１回に１つのデータワードに対して実行される。この説明のために、ジャンブルプロセスが作用するワードは８ビット長（０～２５５の範囲を与える）であるとするが、他のワードサイズでも実行できる。“秘密”データブロック長は、次の鋸歯状波関数に組み込まれる。

※のプロセスで用いられる。

【００２１】上記のプロセスでは、データとキーの間に明確な区別は無いことが分かる。従って、認証に用いられるどの符号列も、上記のプロセスでキーとして用いられる部分を有することができる。逆に、キーと結合されたデータワードは、“認証”符号列と考えられる。各ワードｂ（ｉ）（０≦ｉ≦ｄ－１）は１回に１つそれぞれハッシングされ、ハッシングを“その場で”に行うことができる。ハッシングプロセス自体には、追加のバッファは必要とされない。

【００２２】上述のプロセスで必要とされる操作は、シフト（２０４８による割り算）、切捨て（［］関数およびｍｏｄ２５６関数）、加算、乗算、およびビットごとの排他的ＯＲ演算であるため、基本的な従来のプロセッサで簡単に実行できる。

【００２３】図２のＳＳＤフィールドの初期化プロセスに戻って、ＲＡＮＤＳＳＤシーケンスと、新規のＳＳＤフィールドの作成指示（図２の矢印１００）が移動ステーションで受信されると、図４に従って新規のＳＳＤフィールドが作成される。移動局ユニットは、ＥＳＮ指定、Ａキー、ＲＡＮＤＳＳＤシーケンスを結合して認証符号列（認証ストリング）を形成する。認証符号列はジャンブルブロック１０１（前述）へ導かれ、ジャンブルブロック１０１はＳＳＤフィールドを出力する。ＳＳＤフィールドは２つのサブフィールドから構成される：認証手順に用いられるＳＳＤ－Ａサブフィールド、および音声プライバシー手順およびある信号メッセージの暗号化（後述）に用いられるＳＳＤ－Ｂサブフィールドである。注意すべき点は、上記のようにして形成されたＳＳＤフィールドを再分割することによって、または、最初にＳＳＤフィールドを拡張することによって、さらに多くのＳＳＤサブフィールドを作成することも可能であることである。ＳＳＤフィールド内のビット数を増大させるには、より多くのデータビットから開始するだけでよい。以下に述べるように、これは通常困難ではない。

【００２４】ホームＣＧＳＡプロセッサは、受信されたＭＩＮ２およびＭＩＮ１指定に対応する移動局ユニットのＥＳＮおよびＡキーを知っている。また、送信したＲＡＮＤＳＳＤシーケンスも知っている。従って、ホームＣＧＳＡプロセッサは、移動局ユニットのＳＳＤフィールド生成プロセスと同じことを行うことができる。ＲＡＮＤＳＳＤ信号を、ＥＳＮ指定およびＡキーと連結し、前述のジャンブルプロセスによって、ＣＧＳＡプロセッサは新規のＳＳＤフィールドを生成し、それをＳＳＤ－ＡおよびＳＳＤ－Ｂのサブフィールドに分割する。しかし、ホームプロセッサで生成されたＳＳＤフィールドは検証されねばならない。

【００２５】図２のように、ＳＳＤフィールドの検証は移動局ユニットによって開始される。移動局ユニットはブロック１０２においてランダム要求シーケンス（ＲＡＮＤＢＳシーケンス）を生成し、サーバ基地局（移動局ユニットが位置するエリアをサービスする基地局）を通じてホームＣＧＳＡプロセッサへそれを送信する。図５のように、ホームＣＧＳＡプロセッサは、ＲＡＮＤＢＳ

シーケンス、移動局ユニットのＥＳＮ、ＭＩＮ１指定、新規作成したＳＳＤ－Ａを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。次に、ジャンブルプロセスは、移動局へ送られるハッシングされた認証信号ＡＵＴＨＢＳを生成する。移動局もまた、ＲＡＮＤＢＳシーケンス、ＥＳＮ指定、ＭＩＮ１指定、新規作成したＳＳＤ－Ａを結合し、ジャンブルプロセスで用いられる認証符号列を形成する。移動局は、そのジャンブルプロセスの結果と、ホームＣＧＳＡプロセッサからのハッシングされた認証信号（ＡＵＴＨＢＳ）とを比較する。比較ステップ（ブロック１０４）で一致すると、移動局は、ＳＳＤフィールドのアップデートに成功したことを示す確認メッセージを、ホームＣＧＳＡプロセッサへ送る。一致しない場合には、その比較結果を移動局が送信する。

【００２６】移動局が初期化されても、ＳＳＤフィールドは、ホームＣＧＳＡプロセッサが新規のＳＳＤフィールドを生成することを指示するまで、そのまま保持される。新規のＳＳＤフィールドの作成は例えば、ＳＳＤフィールドが傍受されたことが認められる場合に生じる。そのような場合、ホームＣＧＳＡプロセッサは移動局にもう一つのＲＡＮＤＳＳＤシーケンスを送り、新規のＳＳＤフィールドを生成するように指示する。

【００２７】前述のように、セルラ電話では各基地局から、そのセル内のすべての移動局ユニットのために、種々の情報信号が送信される。図１の構成では、基地局から送信される信号の一つは、ランダムあるいは疑似ランダムシーケンス（ＲＡＮＤシーケンス）である。ＲＡＮＤシーケンスは、移動局ユニットで生成および送信された信号をランダム化する、種々の認証プロセスに用いられる。ＲＡＮＤシーケンスは、記録／再生による攻撃を防ぐために定期的に変更されねばならない。ＲＡＮＤ信号の変更周期の設定方法として、予想される平均通話時間より短く設定する方法がある。従って、通常移動局では、連続する通話に対して異なったＲＡＮＤ信号を用いることになる。

【００２８】本発明の１つの目的によれば、移動局ユニットは、セルに入ったことを検知するとすぐに認証可能なように基地局に登録する。移動局ユニットが認証された場合にのみ、移動局ユニットが発呼すること、あるいは、基地局から移動局ユニットへ呼を転送することができる。

【００２９】移動局ユニットは、登録プロセスを開始すると、基地局によって同報されたＲＡＮＤシーケンスを受信し、そのＭＩＮ１およびＭＩＮ２指定ならびにそのＥＳＮシーケンスを、ハッシュ認証ストリングとともに（平文で）送信する。図６に従って、ＲＡＮＤシーケンス、ＥＳＮシーケンス、ＭＩＮ１指定およびＳＳＤ－Ａサブフィールドを連結して認証ストリングを形成し、その認証ストリングをジャンブルプロセスに送ることによって、、ハッシュ認証ストリングが導出される。ジャンブルプロセスの出力のハッシュ認証ストリングは、ＥＳＮシーケンスとともにサーバ基地局に送られる。

【００３０】ある実施例では、移動局ユニットによって使用されるＲＡＮＤシーケンスの全部または一部もまた（ＥＳＮシーケンスならびにＭＩＮ１およびＭＩＮ２指定とともに）サーバ基地局に送られる。その理由は、ハッシュ認証ストリングが基地局に到達するときまでにＲＡＮＤ値が変化する可能性があるためである。

【００３１】基地局側では、サーバ基地局は、ＲＡＮＤシーケンスを知っており（基地局がそれを作成したため）、また、移動局ユニットが確認したＥＳＮならびにＭＩＮ２およびＭＩＮ１指定をも知っている。しかし、サーバ基地局は、移動局ユニットのＳＳＤフィールドは知らない。サーバ基地局が（ＭＩＮ１およびＭＩＮ２指定から）知っているのは、移動局ユニットのホームＣＧＳＡプロセッサの識別情報である。

【００３２】その結果、認証プロセスは、移動局ユニットのホームＣＧＳＡプロセッサへ、ＭＩＮ１指定、ＥＳＮシーケンス、移動局ユニットが作成し送信したハッシュ認証ストリング、およびサーバ基地局が同報した（そして、移動局ユニットが、作成したハッシュ認証ストリングに組み込んだ）ＲＡＮＤシーケンスを送ることによって進行する。移動局ユニットのＭＩＮ１指定およびＥＳＮシーケンスから、ホームＣＧＳＡプロセッサは、移動局ユニットの識別情報、およびそれによって、移動局ユニットのＳＳＤ－Ａサブフィールドを知る。

【００３３】従って、ホームＣＧＳＡプロセッサは、移動局ユニットがしたのと同じように認証ストリングを作成し、それをジャンブルプロセス（図６）に送ることができる。移動局ユニットのホームＣＧＳＡプロセッサによって作成されたハッシュ認証ストリングが、移動局ユニットで作成されサーバ基地局によって提供されたハッシュ認証ストリングと一致した場合、確認は成功と認められる。このような場合、ホームＣＧＳＡプロセッサはサーバ基地局に移動局ユニットのＳＳＤフィールドを提供する。ちなみに、ＥＳＮ指定およびＳＳＤフィールドを安全に保持するため、基地局とＣＧＳＡプロセッサの間の通信は暗号化形式で実行される。

【００３４】上記のプロトコルでは、移動局ユニットのＣＧＳＡプロセッサは、ハッシュ認証ストリングの正当性の確認を試みる。確認が失敗した場合、ＣＧＳＡプロセッサは、サーバ基地局に対し、移動局ユニットは認証されなかったことを通知し、移動局ユニットとの接続を放棄するか、または、移動局ユニットに登録プロセスの再試行を指示することを提案する。登録プロセスを再試行するためには、ホームＣＧＳＡプロセッサは、認証プロセスへの関与を続行するか、または、それをサーバ基地局に委任することができる。

【００３５】後者の場合、サーバ基地局はホームＣＧＳ

Ａプロセッサに対し移動局ユニットのＥＳＮシーケンスおよびＭＩＮ１指定を通知し、ＣＧＳＡプロセッサは移動局ユニットのＳＳＤフィールドおよびＳＳＤフィールドの作成に使用されたＲＡＮＤＳＳＤを応答する。その後、ハッシュ認証ストリングを作成し、それを移動局ユニットによって送信されたハッシュ認証ストリングと比較するという意味で、認証がサーバ基地局によって実行される。続いて、サーバ局が移動局ユニットにＲＡＮＤＳＳＤを送信することによって、ホームＣＧＳＡプロセスなしで再試行指令が実行可能となる。この「登録」プロトコルを図３に示す。

【００３６】移動局ユニットが（上記のプロセスによって）サーバ基地局に「登録」されると、サーバ基地局は移動局ユニットのＥＳＮおよびＳＳＤフィールドを所有し、そのセルでの以後の認証プロセスは、次の１つの場合を除いてホームＣＧＳＡプロセッサの参照なしにサーバ基地局で実行可能である。何らかの理由で、ＳＳＤフィールドを変更したい場合には、通信はホームＣＧＳＡプロセッサと移動局ユニットの間で有効であり、サーバ基地局はこの通信のための通路としてのみ作用する。その理由は、新たなＳＳＤフィールドの作成は秘密Ａキーへのアクセスを必要とし、ＣＧＳＡプロセッサ以外によるＡキーへのアクセスは全く許されていないためである。

【００３７】従って、新たなＳＳＤフィールドが作成され移動局ユニットがホームＣＧＳＡのエリアに存在しない場合、次のことが起こる。

・　ホームＣＧＳＡプロセッサはＲＡＮＤＳＳＤシーケンスを作成し、そのＲＡＮＤＳＳＤシーケンスに基づいてＳＳＤフィールドを変更する。

・　ホームＣＧＳＡプロセッサはサーバ基地局にＲＡＮＤＳＳＤシーケンスおよび新たに作成したＳＳＤフィールドを提供する。

・　サーバ基地局は、移動局ユニットに対し、ＳＳＤフィールドを変更するよう指示し、移動局ユニットにＲＡＮＤＳＳＤシーケンスを提供する。

・　移動局ユニットはＳＳＤフィールドを変更し、サーバ基地局に要求ストリングを送る。

・　サーバ基地局は（上記の）ＡＵＴＨＢＳストリングを作成し、それを移動局ユニットに送る。

・　移動局ユニットはＡＵＴＨＢＳストリングを確認し、サーバ基地局に対し、移動局ユニットおよびサーバ基地局の両方が同一のＳＳＤフィールドを有することを通知する。

【００３８】サーバ基地局によって登録された後、移動局ユニットは図７の認証プロセスとともに通話を開始することができる。通話開始シーケンスは、信号ＲＡＮＤ、ＥＳＮ、ＳＳＤ－Ａおよび少なくともいくつかの被呼者識別（電話）番号（図７のＭＩＮ３）を連結したものである。連結された信号は、サーバ基地局が確認可能なハッシュ認証シーケンスを生成するためにジャンブルプロセスに送られる。もちろん、サーバ基地局での確認を可能にするためには、被呼者識別情報（および、以前のように、おそらくＲＡＮＤ信号の一部）は基地局が受信可能な方法（例えば平文）で送信されなければならない。認証シーケンスが確認されると、基地局は呼を処理し被呼者への接続を形成することが可能となる。

【００３９】移動局ユニットが「被呼者」である場合に移動局ユニットに接続するためのプロトコルは図６の登録プロトコルに従う。すなわち、サーバ基地局は、被呼移動局に対し、ＲＡＮＤシーケンス、ＥＳＮ指定、ＭＩＮ１指定およびＳＳＤ－Ａサブフィールドから作成された認証シーケンスを送信するよう要求する。認証が実行されると、基地局と被呼者移動局ユニットの間には、被呼者移動局ユニットが発呼移動局ユニット（または固定局ユニット）との間でデータを送受信するためのパスが設定される。

【００４０】上記のすべての認証は、認証されるパケットすなわちストリング自体に関してのみ（確認されるという意味で）有効であることに注意すべきである。その他の場合にセキュリティを強化するためには、３つの異なる付加的なセキュリティ手段が使用可能である。それらは、音声暗号化、臨時の再認証、および制御メッセージ暗号化である。

【００４１】［音声暗号化］

音声信号は、最初にそれをディジタル形式に変換することによって暗号化される。これはさまざまな従来の方法で実現可能であり、圧縮や誤り訂正符号を加えることもできる。ディジタル信号のビットはＫビットからなる連続するグループに分割され、各グループが暗号化される。特に、移動局ユニットおよび基地局の両方において、ＲＡＮＤシーケンス、ＥＳＮおよびＭＩＮ１指定、ならびにＳＳＤ－Ｂサブフィールドは連結されジャンブルプロセスに送られる。

【００４２】ジャンブルプロセスは２Ｋビットを生成し、これらのビットはそれぞれＫビットからなるグループＡおよびＢに分割される。移動局ユニットでは、グループＡが出力音声を暗号化するために使用され、グループＢが入力音声を解読するために使用される。逆に、基地局では、グループＡが入力音声を解読するために使用され、グループＢが出力音声を暗号化するために使用される。図８はこの音声暗号化および解読プロセスを示す。

【００４３】［再認証］

基地局の希望により、基地局によってアクティブであると信じられている移動局ユニットが、実際に、アクティブであると認定された移動局ユニットであることを確認するために、再認証プロセスが開始される。これは、基地局が、移動局ユニットに対し、図９に従ってハッシュ認証ストリングの送信を要求することによって実現され

る。このような各要求とともに、基地局は特殊な（ＲＡＮＤＵ）シーケンスを送信する。移動局ユニットは、ＲＡＮＤＵシーケンス、移動局ユニットのエリアコードＭＩＮ２指定、ＥＳＮ指定、ＭＩＮ１指定およびＳＳＤ－Ａ指定を連結することによって認証ストリングを作成する。連結されたストリングはジャンブルプロセスに送られ、生じたハッシュ認証ストリングが基地局に送られる。基地局は、この時点で、ハッシュ認証ストリングが正当であることを確認することができる。

【００４４】［制御メッセージ暗号化システム］
第３のセキュリティ手段は、制御メッセージのプライバシー（秘密性）の保証を取り扱う。設定された通話の間に、制御メッセージの送信を要求するさまざまな状況が生じることがある。ある場合は、制御メッセージは発呼移動局または基地局に重大な悪影響を与えることがある。このため、対話の進行中に送信されるある種の制御メッセージを（十分に）暗号化することが所望される。あるいは、選択されたメッセージ種の選択されたフィールドを暗号化することも可能である。これは、クレジットカード番号のような「データ」制御メッセージや、通話再定義制御メッセージを含む。これは制御メッセージ暗号化システムによって実現される。

【００４５】制御メッセージ暗号化システム（ＣＭＣ）は以下の性質を有する対称鍵暗号化システムである。
（１）　比較的安全である。
（２）　８ビットコンピュータ上で効率的に動作する。
（３）　自己反転的である。

【００４６】ＣＭＣの暗号鍵は、次のようにして「秘密」（例えば、ＳＳＤ－Ｂサブフィールド）から導出される、２５６バイトの配列ＴＢＯＸ［ｚ］である。
１．　０≦ｚ＜２５６の範囲の各ｚに対し、ＴＢＯＸ［ｚ］＝ｚとおく。
２．　配列ＴＢＯＸ［ｚ］および秘密（ＳＳＤ－Ｂ）をジャンブルプロセスに送る。これは、本質的に、（図８では２５６バイトではなく２Ｋビットであることを除いては）図８の要素３０１、３０２および３０３で示されたものである。

【００４７】鍵が導出されると、ＣＭＣが、制御メッセージを暗号化および解読するために使用可能となる。あるいは、鍵が使用されるたびごとに、鍵を「その場で」導出することも可能である。ＣＭＣは複数バイトの可変長メッセージを暗号化する能力を有する。ＣＭＣの作用は自己反転的、あるいは逆数的である。すなわち、平文を生じるために暗号文に対してなされる操作と、暗号文を生じるために平文に対してなされる操作が、完全に同一である。従って、ＣＭＣ操作を２度実行すると、データは不変のままである。

【００４８】以下の説明では、暗号化プロセス（および解読プロセス）に対し、平文（または暗号文）はデータバッファ内に存在し、ＣＭＣは、そのデータバッファの内容に対し、データバッファの最終内容が暗号文（または平文）を構成するように作用する、と仮定する。これは、図１０の要素５０２および５０４が１つの同一のレジスタでよいことを意味する。

【００４９】ＣＭＣは３つの連続する段階からなり、それぞれデータバッファ内の各バイト列を変更する。データバッファの長さがｄバイトであり、各バイトをｂ（ｉ）で表すとき、０≦ｉ＜ｄの範囲のｉに対し、

Ｉ．ＣＭＣの第１段階は次の通りである。
１．　変数ｚを０に初期化する。
２．　０≦ｉ＜ｄの範囲の連続する整数値ｉに対し、
ａ．　変数ｑを、ｑ＝ｚ（＋）（ｉの下位バイト）とする。ただし、（＋）はビットごとの排他的ＯＲ演算子である。
ｂ．　変数ｋを、ｋ＝ＴＢＯＸ［ｑ］とする。
ｃ．　ｂ（ｉ）を、ｂ（ｉ）＝ｂ（ｉ）＋ｋ　ｍｏｄ　２５６　と更新する。
ｄ．　ｚを、ｚ＝ｂ（ｉ）＋ｚ　ｍｏｄ　２５６　と更新する。

【００５０】ＩＩ．　ＣＭＣの第２段階は、次の通りである。
１．　０≦ｉ＜（ｄ－１）／２の範囲のすべての整数値ｉに対し、ｂ（ｉ）＝ｂ（ｉ）＃（ｂ（ｄ－１－ｉ）ＯＲ　１）　とする。ただし、（＋）はビットごとのＯＲ演算子である。

ＩＩＩ．　ＣＭＣの最終段階は、第１段階の逆である解読である。
１．　変数ｚを０に初期化する。
２．　０≦ｉ＜ｄの範囲の連続する整数値ｉに対し、
ａ．　変数ｑを、ｑ＝ｚ（＋）（ｉの下位バイト）とする。
ｂ．　変数ｋを、ｋ＝ＴＢＯＸ［ｑ］とする。
ｃ．　ｚを、ｚ＝ｂ（ｉ）＋ｚ　ｍｏｄ　２５６　と更新する。
ｄ．　ｂ（ｉ）を、ｂ（ｉ）＝ｂ（ｉ）－ｋ　ｍｏｄ　２５６　と更新する。

【００５１】選択された制御メッセージおよびデータメッセージを暗号化および解読するために使用されるこれら３段階のプロセスを図１０に示す。１つの所望される実施例では、第１段階および第３段階はそれぞれ自動鍵暗号化および解読である。自動鍵システムは、システムの出力が以後のシステムの出力に影響を与えるように使用されるような時変システムである。暗号および自動鍵システムに関するこれ以上のことは、W. Diffie and M. E. Hellman, "Privacy and Authentication:An Introduction to Cryptography"（プライバシーと認証：暗号入門），Proc.of the I.E.E.E., Vol.67, No.3（１９７９年３月）を参照。

【００５２】［移動局ユニット機器］
図１１は、移動局ユニットハードウェアのブロック図で

ある。これは、セルラ電話のキーパッド、受話器および装置の電源制御スイッチ（図示せず）を含む制御ブロック２００を有する。制御ブロック２００はプロセッサ２１０に接続される。プロセッサ２１０は、音声信号をディジタル表現に変換すること、誤り訂正符号を組み込むこと、出力ディジタル音声信号を暗号化すること、入力音声信号を解読すること、さまざまな制御メッセージを形成および暗号化（さらに解読）すること、などのような、移動局ユニットの動作を制御する。

【００５３】ブロック２１０は、信号の送受信に関連する回路の集合からなるブロック２２０に結合される。ブロック２００～２２０は、市販の移動電話装置によって現在実行されている機能を実行する（市販の装置は暗号化および解読は実行しないが）、基本的には従来のブロックである。これまで説明した認証および暗号化プロセスを実現するため、図１１の装置は、プロセッサ２１０に結合したいくつかのレジスタからなるブロック２４０と、同じくプロセッサ２１０に結合した「個性」モジュール２３０をも含む。モジュール２３０は、移動電話装置の物理的構造の一部でもよいし、ソケットインタフェースを通じて移動電話装置に結合した取り外し可能（かつはめ込み可能）なモジュールでもよい。これは、電磁パスすなわち接続を通じてプロセッサ２１０に結合してもよい。要するに、モジュール２３０は、例えば、「スマートカード」である。

【００５４】モジュール２３０はジャンブルプロセッサ２３１およびプロセッサ２３１に付随するいくつかのレジスタからなる。あるいは、他の所望される実施例では、Ａキーのみがモジュール２３０内に存在する。Ａキー、ならびにＭＩＮ１およびＭＩＮ２指定を、ブロック２４０のレジスタではなく、モジュール２３０のレジスタに組み込む（そして保持する）ことからいくつかの利益が生じる。

【００５５】生成されたＳＳＤフィールドをモジュール２３０のレジスタに格納することも有益である。さらに、プロセッサ２３１のプロセスを実行するために必要な作業レジスタをモジュール２３０のレジスタに含めることも有益である。これらの要素をモジュール２３０に含めることにより、ユーザは、モジュールを携帯してそれを異なる移動局ユニット（例えば「拡張」移動局ユニット）で使用するとともに、重要な情報がモジュール外に格納されることがないようにすることができる。もちろん、移動局ユニットは、モジュール２３０が装置の統合的かつ永続的部分であるように生産することも可能である。このような実施例では、ジャンブルプロセッサ２３１はプロセッサ２１０内に合併することができる。ブロック２４０は、装置のＥＳＮ指定および受信されるさまざまなＲＡＮＤシーケンスを格納する。

【００５６】上記の説明はセルラ電話環境における加入者認証について述べられており、携帯用ポケット受話器に使用される個人通信ネットワークを含むものであるが、本発明の原理は、通信が十分に安全ではないと認識され、模写が潜在的問題であるような他の状況における利用可能性を有することは明らかである。これには例えばコンピュータネットワークが含まれる。

【００５７】

【発明の効果】以上述べたごとく、本発明によれば、現在セルラ電話で使用される種類のハードウェアを使用して、高速で効率的に実行可能な公開鍵認証方式が与えられる。

【図面の簡単な説明】

【図１】固定および移動電話の両方のサービスのために相互接続された、ネットワーク提供者およびセルラ無線提供者の構成を示す図である。

【図２】共有秘密データフィールドの作成と同一性の検証を行うプロセスを示す図である。

【図３】例えば移動局ユニットが最初に基地局によってサービスされるセルに入った場合の、訪問先の基地局における登録プロセスを示す図である。

【図４】共有秘密データを作成するために連結されハッシュされた要素を示す図である。

【図５】確認シーケンスを作成するために連結されハッシュされた要素を示す図である。

【図６】移動局ユニットが発信する際に、登録シーケンスを作成するために連結されハッシュされた要素を示す図である。

【図７】発呼シーケンスを作成するために連結されハッシュされた要素を示す図である。

【図８】移動局ユニットにおける音声暗号化および解読のプロセスを示す図である。

【図９】再認証シーケンスを作成するために連結されハッシュされた要素を示す図である。

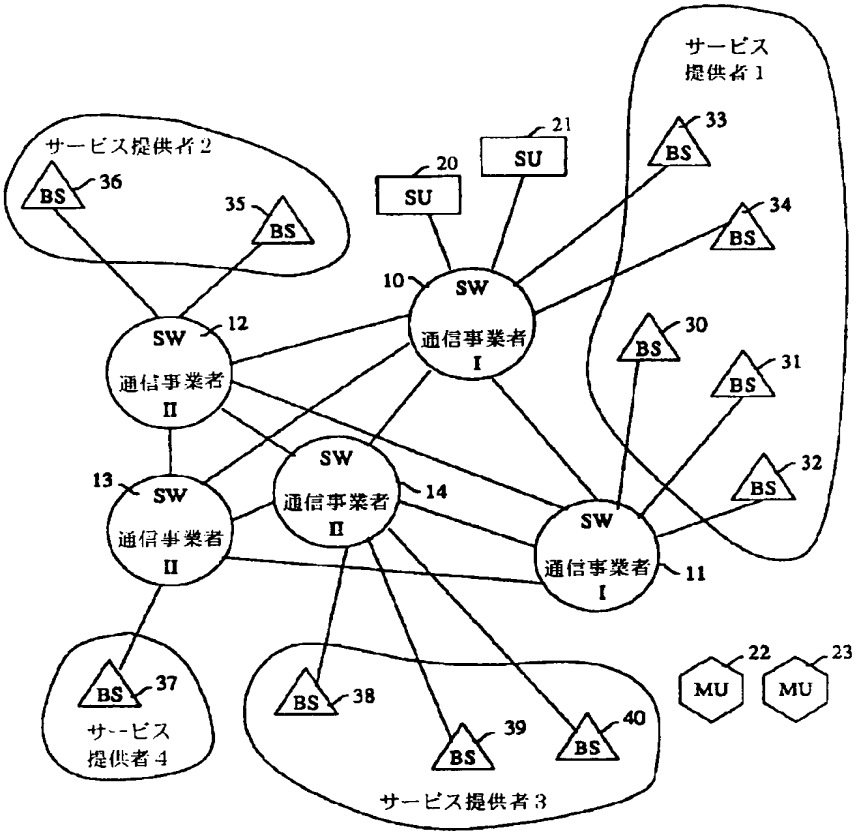
【図１０】選択された制御メッセージおよびデータメッセージを暗号化および解読するための３段プロセスを示す図である。

【図１１】移動局ユニットのハードウェアのブロック図である。

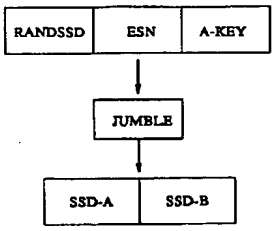
【符号の説明】

１０－１４　交換機
２０－２１　固定局
２２－２３　移動局
３０－４０　基地局
１０１　ジャンブルブロック
２００　制御ブロック
２１０　プロセッサ
２２０　送受信ブロック
２３０　モジュール
２３１　プロセッサ
２４０　レジスタブロック

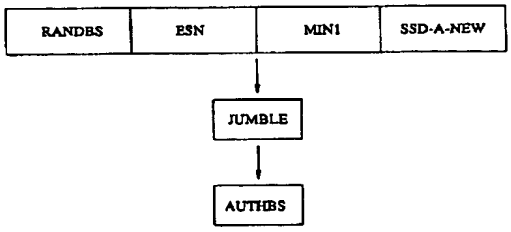
【図１】


サービス
提供者１
サービス提供者２
SU
SU
BS
BS
BS
BS
BS
BS
BS
BS
BS
BS
SW
通信事業者
I
SW
通信事業者
II
SW
通信事業者
II
SW
通信事業者
II
SW
通信事業者
I
MU
MU
サービス
提供者４
サービス提供者３
10
11
12
13
14
20
21
22
23
30
31
32
33
34
35
36
37
38
39
40

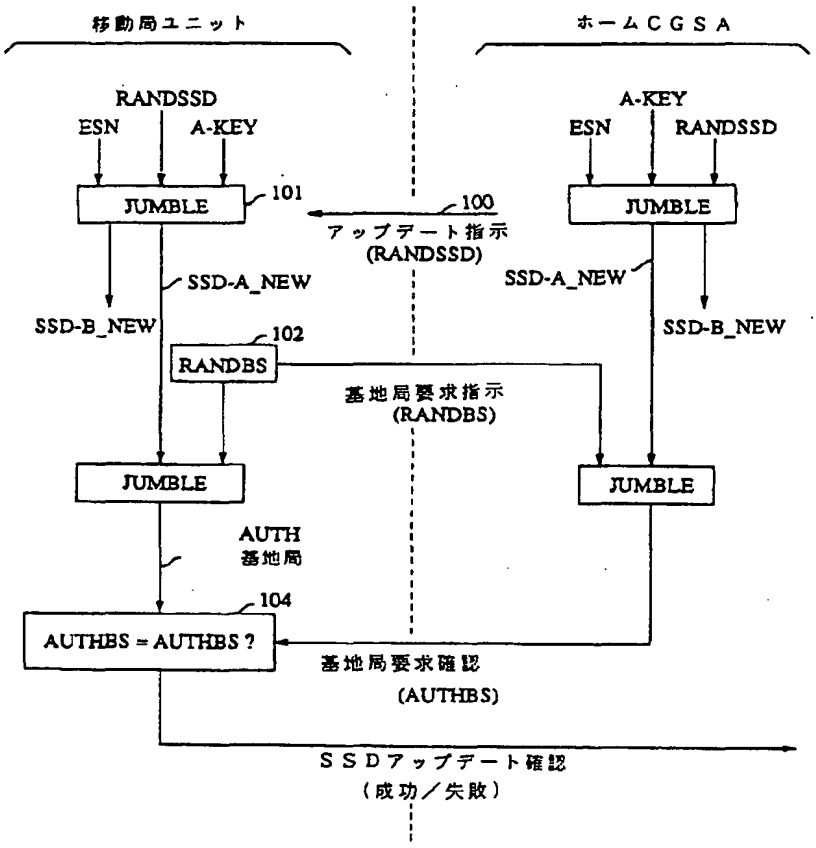
【図４】


RANDSSD
ESN
A-KEY
JUMBLE
SSD-A
SSD-B

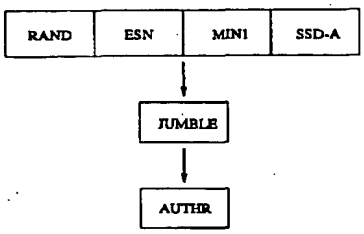
【図５】


RANDBS
ESN
MIN1
SSD-A-NEW
JUMBLE
AUTHBS

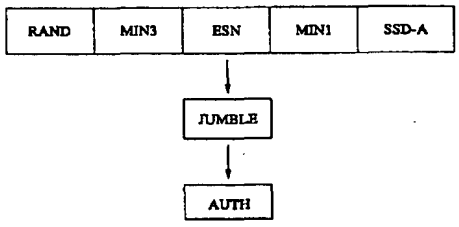
【図２】


移動局ユニット
ホームＣＧＳＡ
RANDSSD
ESN
A-KEY
A-KEY
ESN
RANDSSD
JUMBLE
101
100
JUMBLE
アップデート指示
(RANDSSD)
SSD-A_NEW
SSD-A_NEW
SSD-B_NEW
SSD-B_NEW
102
RANDBS
基地局要求指示
(RANDBS)
JUMBLE
JUMBLE
AUTH
基地局
104
AUTHBS = AUTHBS ?
基地局要求確認
(AUTHBS)
ＳＳＤアップデート確認
（成功／失敗）

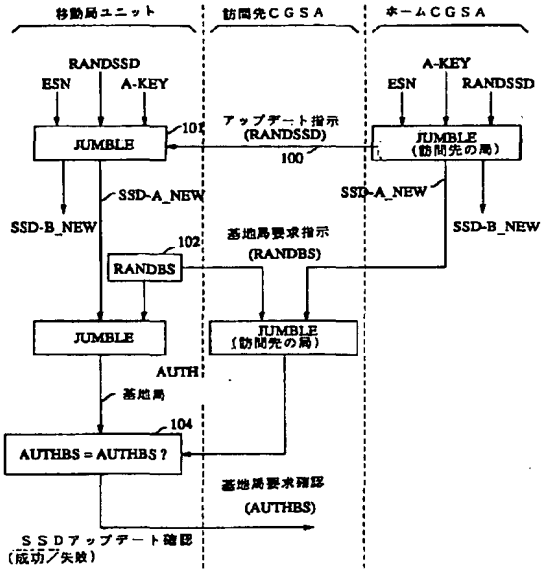
【図６】


RAND
ESN
MIN1
SSD-A
JUMBLE
AUTHR

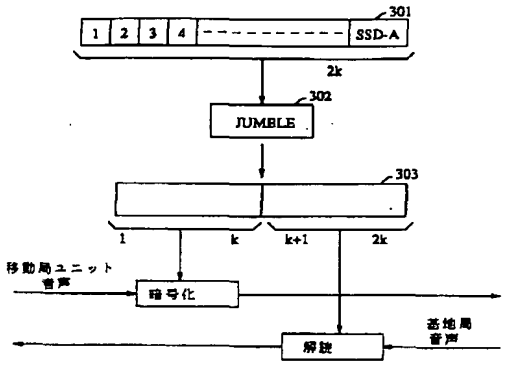
【図７】


RAND
MIN3
ESN
MIN1
SSD-A
JUMBLE
AUTH

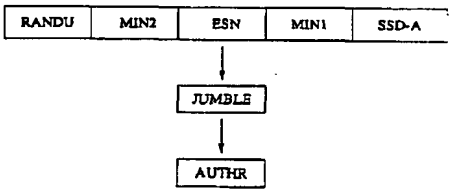
【図３】


移動局ユニット
訪問先ＣＧＳＡ
ホームＣＧＳＡ
RANDSSD
ESN
A-KEY
A-KEY
ESN
RANDSSD
JUMBLE
101
アップデート指示
(RANDSSD)
100
JUMBLE
(訪問先の局)
SSD-A_NEW
SSD-A_NEW
SSD-B_NEW
SSD-B_NEW
基地局要求指示
(RANDBS)
102
RANDBS
JUMBLE
JUMBLE
(訪問先の局)
AUTH
基地局
104
AUTHBS = AUTHBS ?
基地局要求確認
(AUTHBS)
ＳＳＤアップデート確認
(成功／失敗)

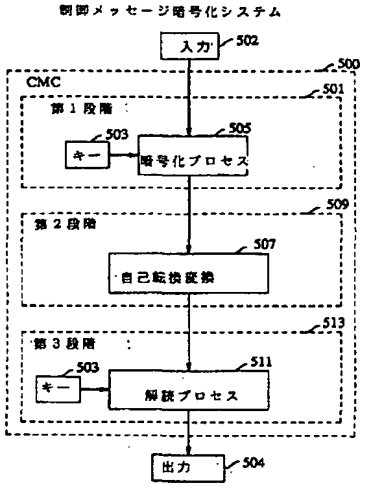
【図８】


301
1
2
3
4
SSD-A
2k
302
JUMBLE
303
1
k
k+1
2k
移動局ユニット
音声
暗号化
基地局
音声
解読

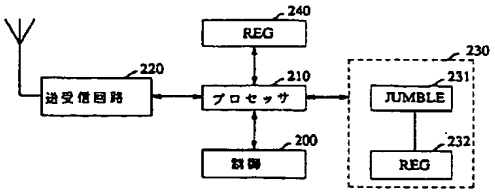
【図９】


RANDU
MIN2
ESN
MIN1
SSD-A
JUMBLE
AUTHR

【図１０】


制御メッセージ暗号化システム
入力
502
500
CMC
501
第１段階
503
キー
505
暗号化プロセス
509
第２段階
507
自己転換変換
513
第３段階
503
キー
511
解読プロセス
出力
504

【図１１】



フロントページの続き

(72)発明者　フィリップ　アンドリュー　トラヴァンティ
アメリカ合衆国　07974　ニュージャージー　マーレー　ヒル、キャンドルウッド　ドライヴ　15